

72
3-1789
Docket No. 1080.1067/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Kenichi UTSUMI, et al.

Serial No.: To Be Assigned

Filed: November 9, 1998

For: LICENSE DEVOLUTION APPARATUS

Group Art Unit: To Be Assigned

Examiner: To Be Assigned



**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

*Assistant Commissioner for Patents
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 10-138663 filed May 20, 1998.

It is respectfully requested that Applicants be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,
STAAS & HALSEY

Dated: November 9, 1998

By:


James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

U.S. PRO
09/187749
11/09/98

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
this Office.

願 年 月 日
Date of Application:

1998年 5月20日

願 番 号
Application Number:

平成10年特許願第138663号

願 人
Applicant(s):

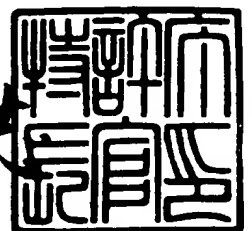
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1998年10月23日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



【書類名】 特許願

【整理番号】 9890314

【提出日】 平成10年 5月20日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明の名称】 ライセンス委譲装置

【請求項の数】 7

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 内海 研一

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 平野 秀幸

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小谷 誠剛

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100094330

 【弁理士】

 【氏名又は名称】 山田 正紀

【手数料の表示】

 【予納台帳番号】 017961

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704376

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ライセンス委譲装置

【特許請求の範囲】

【請求項 1】 所定の鍵により暗号化されたコンテンツと、自分を特定する第 1 のメディア ID と、前記鍵と該コンテンツの使用権を表す第 1 の使用権情報との双方が一緒あるいは別々に前記第 1 のメディア ID で暗号化されてなる第 1 の暗号化セキュア情報とが格納された第 1 の記憶媒体と、自分を特定する第 2 のメディア ID が格納された第 2 の記憶媒体とをアクセスして前記第 1 の記憶媒体に格納されたコンテンツの使用権を前記第 1 の記憶媒体から前記第 2 の記憶媒体に委譲するライセンス委譲装置において、

前記コンテンツの使用権の委譲にあたり前記第 1 の記憶媒体に格納された第 1 の暗号化セキュア情報を前記第 1 のメディア ID を用いて復号化することにより前記鍵と前記第 1 の使用権情報とを得る復号化手段、および

前記復号化手段による復号化により得られた鍵と、前記復号化手段による復号化により得られた第 1 の使用権情報があらかず第 1 の使用権が譲渡あるいは分与された第 2 の使用権をあらわす第 2 の使用権情報との双方を一緒あるいは別々に前記第 2 のメディア ID で暗号化することにより第 2 の暗号化セキュア情報を生成して前記第 2 の記憶媒体に格納させる暗号化手段を備えたことを特徴とするライセンス委譲装置。

【請求項 2】 前記暗号化手段が、さらに、前記第 1 の使用権から前記第 2 の使用権を差し引いた後の第 3 の使用権をあらわす第 3 の使用権情報を、あるいは前記鍵と該第 3 の使用権情報との双方を、前記第 1 のメディア ID で暗号化して前記第 1 の記憶媒体に書き戻すことにより、該第 1 の記憶媒体に、前記第 1 の暗号化セキュア情報に代えて、前記鍵と前記第 3 の使用権情報との双方が該第 1 のメディア ID で暗号化されてなる第 3 の暗号化メディア情報を格納させるものであることを特徴とする請求項 1 記載のライセンス委譲装置。

【請求項 3】 前記第 1 の記憶媒体が持つ前記コンテンツの使用権全体を前記第 2 の記憶媒体に委譲する場合に、前記暗号化手段が、前記復号化手段による復号化により得られた鍵と、前記第 1 の使用権の全てを受け継いだ第 2 の使用権

をあらわす第2の使用権情報とが暗号化されてなる第2の暗号化セキュア情報を生成して前記第2の記憶媒体に格納させるとともに、前記第1の記憶媒体に格納されている前記第1の暗号化セキュア情報を構成する前記鍵を破壊させるものであることを特徴とする請求項1記載のライセンス委譲装置。

【請求項4】 コンテンツの使用権委譲前において、前記第1の記憶媒体が、暗号化された、使用権を委譲しようとするコンテンツが格納されたものであって、

コンテンツの使用権の委譲にあたり、前記第1の記憶媒体に格納された、委譲対象の暗号化されたコンテンツを読み出して、暗号化された状態のまま、前記第2の記憶媒体に格納するコンテンツ移動手段を備えたことを特徴とする請求項1記載のライセンス委譲装置。

【請求項5】 前記第1の使用権情報および前記第2の使用権情報が使用権が存在することをあらわすものであり、前記第3の使用権情報が使用権が存在しないことをあらわすものであることを特徴とする請求項1記載のライセンス委譲装置。

【請求項6】 前記第1の使用権情報が、第1の使用可能回数あるいは使用可能時間をあらわすものであり、前記第2の使用権情報が、該第1の使用可能回数あるいは使用可能時間以内の第2の使用可能回数あるいは使用可能時間をあらわすものであり、前記第3の使用権情報が、該第1の使用可能回数あるいは使用可能時間から該第2の使用可能回数あるいは使用可能時間を差し引いた後の第3の使用可能回数あるいは使用可能時間をあらわすものであることを特徴とする請求項1記載のライセンス委譲装置。

【請求項7】 前記第1の記憶媒体および前記第2の記憶媒体をそれぞれ駆動する第1のドライブおよび第2のドライブを備えるとともに、該第1のドライブおよび該第2のドライブが、前記第1の記憶媒体および前記第2の記憶媒体それぞれをアクセスする、それぞれ第1のファームウェアおよび第2のファームウェアを備えたものであり、

前記復号化手段および前記暗号化手段が、前記第1のファームウェアと前記第2のファームウェアとの複合体としてのファームウェア内に構成されたものであ

って、

前記第 1 のファームウェアのみが前記第 1 のドライブにより駆動される前記第 1 の記憶媒体をアクセスする権原を有するとともに、前記第 2 のファームウェアのみが前記第 2 のドライブにより駆動される第 2 の記憶媒体をアクセスする権原を有するものであることを特徴とする請求項 1 記載のライセンス委譲装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンテンツの使用権を第 1 の記憶媒体から第 2 の記憶媒体に委譲するライセンス委譲装置に関する。

【0002】

【従来の技術】

近年、如何にして著作権の保護の実効を図るかが問題となってきている。

例えば本のような有形物の場合、頒布すること自体は複製を伴わず、本を転売すればその本は購入者の手もとに渡り販売者のもとには本は存在しなくなり、したがって著作権の保護は比較的簡単であるが、デジタル情報化された著作物の場合、例えばそのデジタル化された著作物をネットワークを介して送信すると自分側と相手側との双方に同じ著作物が発生し、頒布すること自体が複製を伴う結果となり、通常、このようなデジタル情報化された著作物に対する著作権の実効的な保護は極めて難しいとされている。

【0003】

【発明が解決しようとする課題】

本発明は、上記事情に鑑み、デジタル化された文書、映画、プログラム等のコンテンツの使用権を、そのコンテンツに関し権利を有する者の保護を図りつつ委譲することのできるライセンス委譲装置を提供することを目的とする。

【0004】

【課題を解決するための手段】

上記目的を達成する本発明のライセンス委譲装置は、

所定の鍵により暗号化されたコンテンツと、自分を特定する第 1 のメディア I

Dと、上記鍵とそのコンテンツの使用権を表す第1の使用情報との双方が一緒あるいは別々に第1のメディアIDで暗号化されてなる第1の暗号化セキュア情報とが格納された第1の記憶媒体と、自分を特定する第2のメディアIDが格納された第2の記憶媒体とをアクセスして第1の記憶媒体に格納されたコンテンツの使用権を第1の記憶媒体から第2の記憶媒体に委譲するライセンス委譲装置において、

コンテンツの使用権の委譲にあたり第1の記憶媒体に格納された第1の暗号化セキュア情報を第1のメディアIDを用いて復号化することにより上記鍵と上記第1の使用権情報とを得る復号化手段、および

上記復号化手段による復号化により得られた鍵と、および上記復号化手段による復号化により得られた第1の使用権情報があわす第1の使用権が譲渡あるいは分与された第2の使用権をあらわす第2の使用権情報との双方を一緒にあるいは別々に上記第2のメディアIDで暗号化することにより第2の暗号化セキュア情報を生成して第2の記憶媒体に格納させる暗号化手段を備えたことを特徴とする。

【0005】

ここで、上記本発明のライセンス委譲装置において、上記暗号化手段は、さらに、上記第1の使用権から上記第2の使用権を差し引いた後の第3の使用権をあらわす第3の使用権情報を、あるいは鍵と上記第3の使用権情報との双方を、上記第1のメディアIDで暗号化して第1の記憶媒体に書き戻すことにより、第1の記憶媒体に、上記第1の暗号化セキュア情報に代えて、上記鍵と上記第3の使用権情報との双方が第1のメディアIDで暗号化されてなる第3の暗号化メディア情報を格納させるものであってもよく、あるいは、第1の記憶媒体が持つ上記コンテンツの使用権全体を第2の記憶媒体に委譲する場合に、上記暗号化手段は、上記復号化手段による復号化により得られた鍵と、上記第1の使用権の全てを受け継いだ第2の使用権をあらわす第2の使用権情報とが暗号化されてなる第2の暗号化セキュア情報を生成して第2の記憶媒体に格納させるとともに、第1の記憶媒体に格納されている第1の暗号化セキュア情報を構成する鍵を破壊させるものであってもよい。

【0006】

尚、上記の、「鍵と、……第1の使用権情報との双方が一緒にあるいは別々に第1のメディアIDで暗号化されてなる第1の暗号化セキュア情報」は、鍵を第1のメディアIDで暗号化し、これとは別に第1の使用権情報を第1のメディア情報で暗号化し、それらの暗号化された鍵と暗号化された第1の使用権情報とを合わせたものを第1の暗号化セキュア情報と称してもよく、あるいは、鍵と第1の使用権情報との双方を連ねたものを第1のメディア情報で暗号化し、その暗号化された情報を第1の暗号化セキュア情報と称してもよいことを意味している。

【0007】

また、上記の、「鍵と、……第2の使用権情報の双方を一緒にあるいは別々に……第2のメディアIDで暗号化することにより第2の暗号化セキュア情報を生成して……」や「鍵と、……第3の使用権情報との双方が第1のメディアIDで暗号化されてなる第3の暗号化セキュア情報」も同様である。

さらに、上記の、「第3の使用権情報を、あるいは……鍵と……第3の使用権情報との双方を、……第1のメディアIDで暗号化して……」は、鍵と、第1の使用権情報あるいは第2の使用権情報を別々に暗号化するシステムにおいては、第3の使用権情報のみを暗号化すればよく、鍵と第1（あるいは第2）の使用権情報を連ねたものを暗号化するシステムにおいては、鍵と第3の使用権情報との双方を連ねたものを暗号化することを意味している。

【0008】

本発明のライセンス委譲装置は、例えばMO（光磁気ディスク）やハードディスクには、それぞれに固有のID（メディアIDと称する）が付されている点に着目し、完成されたものである。

所定の鍵で暗号化されたコンテンツを流通させることによりその暗号化されたコンテンツ自体はその鍵を用いて復号化しない限り使用不可能である。そこで、その暗号化されたコンテンツを復号化するための鍵と、使用権情報（例えばそのコンテンツの使用が許可されているか否かという情報など）との双方を、その記憶媒体独自のメディアIDで暗号化しておく。こうすることにより、その暗号化されたコンテンツは、そのコンテンツがもともと格納された記憶媒体を離れてそ

れ自体が頒布されても使用不能であり、鍵もそのまま頒布したのでは頒布を受けた先ではメディアIDが異なるため鍵を復号化することはできず、したがって使用権のない者による無断使用が防止できる。

【0009】

このようなシステムにおいて、自分（第1の記憶媒体）の使用権を委譲先（第2の記憶媒体）に譲り渡すには、自分（第1の記憶媒体）のメディアIDで鍵および自分の使用権情報を復号化し、自分の使用権の範囲（例えば使用可能な残存回数）の中で使用権を分与し（あるいはその使用権全体であってもよい）、鍵と、その分与されたあるいは全体としての使用権情報を、委譲先（第2の記憶媒体）のメディアID（第2のメディアID）で暗号化してその委譲先（第2の記憶媒体）に格納させる。自分（第1の記憶媒体）には、残りの使用権（使用権が存在しないという使用権を含む）を自分（第1の記憶媒体）のメディアID（第1のメディアID）で暗号化して自分（第1の記憶媒体）に書き戻す。あるいは使用権の全部を委譲する場合は、自分（第1の記憶媒体）では、残りの使用権（この場合は使用権が存在しないという使用権）を暗号化して書き戻す代わりに、自分（第1の記憶媒体）に暗号化された形式で格納されている鍵を破壊してしまってもよい。こうすることにより、そのコンテンツに関し権利を有する者の権利を犯すことなく使用権の譲渡が可能となる。

【0010】

ここで、上記本発明のライセンス委譲装置は、コンテンツの使用権委譲前において、第1の記憶媒体が、暗号化された、使用権を委譲しようとするコンテンツが格納されたものであって、

コンテンツの使用権の委譲にあたり、第1の記憶媒体に格納された、委譲対象の暗号化されたコンテンツを読み出して、暗号化された状態のまま、第2の記憶媒体に格納するコンテンツ移動手段を備えることが好ましい。

【0011】

コンテンツ自体は暗号化された状態のまま頒布されるので、いつ頒布してもよく、例えば既に頒布されているときは鍵と使用権のみを渡せばよいが、例えば上記のコンテンツ移動手段を備えて、コンテンツの使用権の委譲にあたりそのコン

テンツを第1の記憶媒体から第2の記憶媒体に移動（複製）してもよい。

また、上記本発明のライセンス委譲装置において、上記第1の使用権情報および上記第2の使用権情報が使用権が存在することをあらわすものであり、上記第3の使用権情報が使用権が存在しないことをあらわすものであってもよく、あるいは、上記第1の使用権情報が、第1の使用可能回数あるいは使用可能時間をあらわすものであり、上記第2の使用権情報が、その第1の使用可能回数あるいは使用可能時間以内の第2の使用可能回数あるいは使用可能時間をあらわすものであり、上記第3の使用権情報が、第1の使用可能回数あるいは使用可能時間から第2の使用可能回数あるいは使用可能時間を差し引いた後の第3の使用可能回数あるいは使用可能時間をあらわすものであってもよい。

【0012】

このほか、例えば使用権を有する人を特定するIDを使用権情報としてもよく、使用権情報は、使用権の有無や範囲をあらわす情報であればどのような情報であってもよい。

また、上記本発明のライセンス委譲装置において、第1の記憶媒体および第2の記憶媒体をそれぞれ駆動する第1のドライブおよび第2のドライブを備えるとともに、第1のドライブおよび第2のドライブが、第1の記憶媒体および第2の記憶媒体それぞれをアクセスする、それぞれ第1のファームウェアおよび第2のファームウェアを備えたものであり、

上記復号化手段および上記暗号化手段が、上記第1のファームウェアと上記第2のファームウェアとの複合体としてのファームウェア内に構成されたものであって、

上記第1のファームウェアのみが第1のドライブにより駆動される第1の記憶媒体をアクセスする権原を有するとともに、上記第2のファームウェアのみが第2のドライブにより駆動される第2の記憶媒体をアクセスする権原を有するものであることが好ましい。

【0013】

ここで、「第1のファームウェアのみが……第1の記憶媒体をアクセスする権原を有する」、「第2のファームウェアのみが……第2の記憶媒体をアクセスす

る権原を有する」は、例えばアプリケーションプログラム等からは、それら第1のファームウェアや第2のファームウェアを介在させずに直接には第1の記憶媒体や第2の記憶媒体をアクセスすることはできないように構成されていることを意味し、このような構成を備えると以下のような場合を含め、コンテンツに関する正当な権利を有する者の権利が一層確実に保護されることになる。

【0014】

すなわち、仮に、ファームウェアを介在させずにアプリケーションプログラムから直接に記憶媒体をアクセスすることができるシステムの場合、第1の記憶媒体から第2の記憶媒体に使用権を委譲する前にアプリケーションプログラムで第1の記憶媒体を直接にアクセスして上述した第1の暗号化セキュア情報を読み出して第3の記憶媒体に格納しておく。このような前準備を行なった上で使用権を第1の記憶媒体から第2の記憶媒体に委譲する。その委譲が終了した後、再びアプリケーションプログラムで第1の記憶媒体を直接にアクセスして第3の記憶媒体にあらかじめ複製しておいた委譲前の第1の暗号化セキュア情報を第1の記憶媒体に書き戻す。この場合、第1の記憶媒体は使用権を委譲する前の状態に戻り、かつ第2の記憶媒体にも使用権が発生し、正当な権利者の権利が犯される結果をもたらす。

【0015】

そこで、上記のようにファームウェアのみからアクセスを可能とすることにより、上記のような不正の発生を未然に防止することができ、正当な権利者の権利をより一層確実に保護することができる。

【0016】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

ここでは解り易さのため、概念的な実施形態について先ず説明し、次いで具体的な実施形態について説明する。

図1は、本発明のライセンス委譲装置の一実施形態を示す構成図、図2は、その説明のための模式図である。

【0017】

図1には、第1の記憶媒体10、ドライブ20、および第2の記憶媒体30が示されている。第1の記憶媒体10および第2の記憶媒体30は、いずれも、その記憶媒体の種類を問うものではないが、その記憶媒体を特定するメディアIDを有することが必要である。このメディアIDは、同種の記憶媒体を互いに確実に識別するものである必要はなく、例えば同一のメディアIDを持つ2つの記憶媒体が出会うことがほとんど期待できない程度にその記憶媒体にユニークなものであればよい。

【0018】

ドライブ20は、本実施形態では、第1の記憶媒体10を駆動する第1のドライブ、例えば第1の記憶媒体10がMO（光磁気ディスク）の場合の光磁気ディスクドライブ装置と、第2の記憶媒体30を駆動する第2のドライブ、例えば第2の記憶媒体30がハードディスクの場合そのハードディスクを駆動するハードディスクドライブ装置との複合体として観念される。

【0019】

また、第1のドライブには、そのマイクロコンピュータとそのマイクロコンピュータで動作するソフトウェアとの組合せからなる、第1のドライブにより駆動される第1の記憶媒体をアクセスするための第1のファームウェアが搭載されており、これと同様に、第2のドライブにも、マイクロコンピュータとそのマイクロコンピュータで動作するソフトウェアとの組合せからなる、その第2のドライブにより駆動される第1の記憶媒体をアクセスするための第2のファームウェアが搭載されている。ここでは、第1のファームウェアと第2のファームウェアとの複合体としてのファームウェアがドライブ20に搭載されているものと観念する。

【0020】

第1の記憶媒体10および第2の記憶媒体20は、それぞれ、自分自身のメディアIDを記憶しておくMIDエリア11、31、使用権情報やその他コンテンツの属性に関する情報が格納されるセキュアエリア12、32、およびコンテンツ自身が格納されるユーザエリア13、33を有する。ここでは、第1の記憶媒体10が持っているコンテンツの使用権を第2の記憶媒体30に委譲しようとし

ており、したがってここでは、第1の記憶媒体10のMIDエリア11，セキュアエリア12，およびユーザエリア13には、それぞれ、その第1の記憶媒体10のメディアID、使用権情報やその他の属性、およびコンテンツが実際に格納されているものとする。

【0021】

一方、第2の記憶媒体30のMIDエリア31には、その第2の記憶媒体30のメディア30のメディアIDが格納されているが、セキュアエリア32、およびユーザエリア33はあらかじめ領域として用意されていてもよく、あるいは、コンテンツの使用権の委譲にあたってそれらの領域が生成されるものであってもよい。

【0022】

以下において説明する復号化手段21，暗号化手段22，およびコンテンツ移動手段23は、ドライブ20内に搭載されたファームウェア内に構築されており、アプリケーションプログラムは、そのファームウェアを起動することはできるが、そのファームウェアの動作の内部に入り込んでそのファームウェアの動作を制御したり、あるいはそのファームウェアを介在させずに第1の記憶媒体や第2の記憶媒体を直接にアクセスすることはできないように構成されている。

【0023】

つまり、MIDエリア11，31は、ファームウェアによるリードが許可されライトが禁止されているエリアであり、アプリケーションは、ファームウェアを介在させた場合を含めて原則としてMIDエリア11，31へのアクセスが禁止されている。

また、セキュアエリア12，32とユーザエリア13，33はファームエリアによるリード・ライトが許可されているエリアであり、アプリケーションは、本実施形態では、ファームエリアを介在させた場合にのみセキュアエリア12，32とユーザエリア13，33にアクセスすることができ、直接リード・ライトを行うことはできない。但し、ユーザエリア13，33については、アプリケーションによる直接的なアクセスが許可されたエリアであってもよい。

【0024】

尚、MIDエリア11, 31については、セキュアエリア12, 32およびユーザエリア13, 33とは独立に物理的に書き換え不可能な不揮発性の記憶媒体上に設けられていることが望ましい。但し、本実施形態ではMIDエリアはセキュアエリアおよびユーザエリアとともに第1の記憶媒体および第2の記憶媒体上に設けられている。

【0025】

ここで、図2に示すように、第1の記憶媒体10のユーザエリア13に格納されたコンテンツは、鍵1で暗号化された形式で格納されており、その鍵1は、使用権情報41とともに、MIDエリア11に格納された、この第1の記憶媒体10のメディアIDからなる鍵2で暗号化された形式で、セキュアエリア12に格納されている。ここで、図2には、セキュアエリア12に格納された使用権情報41として、‘1→0’が示されているが、‘1’はそのコンテンツの使用権が存在することを意味し、‘0’はそのコンテンツの使用権が無いことを意味し、‘1→0’は、使用権の委譲前は‘1’であって、使用権委譲の際に‘0’に書き換えられることを意味している。また、図2において、セキュアエリア12およびユーザエリア13は、右にさらに延びるように描かれているが、これは、1つの記憶媒体（ここでは第1の記憶媒体10）のユーザエリアに複数のコンテンツが格納され、それら複数のコンテンツそれぞれについて鍵や使用権情報等がセキュアエリア12に格納される場合があることを意味している。

【0026】

ここで鍵1と使用権情報41を鍵2で暗号化するにあたっては、この図2では、鍵1と使用権情報41とを合わせた情報が鍵2で暗号化されているように描かれてれているが、そうであってもよく、あるいは、鍵1が鍵2で暗号化され、それとは別に、使用権情報41が鍵2で暗号化されていてもよい。いずれの場合であっても、鍵2で暗号化された鍵1と、鍵2で暗号化された使用権情報との双方を合わせたものを、ここでは暗号化セキュア情報（本発明にいう第1の暗号化セキュア情報）と称する。

【0027】

コンテンツの使用権の委譲にあたり、図1に示すドライブ20の復号化手段2

1により、第1の記憶媒体10のMIDエリア11に記憶された、第1の記憶媒体10のメディアID（本発明にいう第1のメディアID）からなる鍵2で、セキュアエリア12に格納された第1の暗号化セキュア情報が復号化され、その暗号化により平文の鍵1と使用権情報41（ここでは、使用権が存在することを表わす‘1’）が取り出される。そこで、今度は、図1に示すドライブ20の暗号化手段22により、その復号化により平文に戻された鍵1と使用権情報41（使用権が存在することをあらわす‘1’）が今度は、第2の記憶媒体30のMIDエリア31に格納されたメディアID（本発明にいう第2のメディアID）からなる鍵3で暗号化されて第3の暗号化セキュア情報が生成され、第2の記憶媒体30のセキュアエリア32に格納される。図2における第2の記憶媒体30のセキュアエリア32に描かれた使用権情報42が‘0→1’となっているのは、使用権の委譲を受ける前は使用権が存在せず‘0’であって、使用権の委譲を受けることにより使用権が存在することをあらわす‘1’に書き換えられたことを意味する。

【0028】

また、第1の記憶媒体10には、復号化された使用権情報41が、使用権が存在しないことをあらわす‘0’に書き換えられ、復号化された鍵1と、使用権が存在しないことをあらわす使用権情報が、第1の記憶媒体10のメディアIDからなる鍵2で暗号化されて、新たな暗号化セキュア情報（本発明にいう第3のセキュア情報）が生成され、それまで第1の記憶媒体10のセキュアエリア12に格納されていた第1の暗号化セキュア情報に代えて、その新たに生成された第3のセキュア情報がそのセキュアエリア12に格納される。

【0029】

あるいは、第1の記憶媒体10にはそのコンテンツの使用権が存在しなくなったのであるから鍵1は不要であり、第3のセキュア情報を生成して第1の記憶媒体10のセキュアエリア12に格納することに代え、そのセキュアエリア12に暗号化された形式で格納されている鍵1を破壊してしまってもよい。

また、第1の記憶媒体10のユーザエリア13に格納されている、鍵1で暗号化されたコンテンツは、図1に示すドライブ20のコンテンツ移動手段23によ

り、第1の記憶媒体10から読み出され、鍵1により暗号化された状態のまま、第2の記憶媒体33のユーザエリア33に格納される。

【0030】

以上により、それまで第1の記憶媒体10が所有していた、コンテンツの使用権が、第2の記憶媒体20に委譲される。

それ以降、第2の記憶媒体20を駆動する第2のドライブでは、アプリケーションプログラムからの、このコンテンツの読出し要求があると、その第2のドライブに搭載された第2のファームウェアは、第2の記憶媒体30をアクセスし、その第2の記憶媒体30のMIDエリア31に格納された、その第2の記憶媒体30のメディアIDからなる鍵3で、セキュアエリア32に格納された暗号化セキュア情報を復号化し、使用権が存在することを確認し、鍵1により、ユーザエリア33に格納された、暗号化されたコンテンツを復号化し、その復号化されたコンテンツをアプリケーションプログラムに戻す。

【0031】

一方、その使用権を委譲した後は、第1の記憶媒体10を駆動する第1のドライブでは、仮に、アプリケーションプログラムからの、その使用権を委譲したコンテンツの読み出し要求があった場合、その第1のドライブに搭載された第1のファームウェアは、第1の記憶媒体10をアクセスし、その第1の記憶媒体のMIDエリアに格納された、その第1の記憶媒体30のメディアIDからなる鍵2で、そのセキュアエリア12に格納された暗号化セキュア情報を復号化し、使用権の存在を確認したところ使用権が存在しないことを認識し、あるいは、上述の、鍵1を破壊するシステムの場合は、鍵1が破壊されていること、あるいはそのコンテンツを復号化できないことを認識し、アプリケーションプログラムに対し、そのコンテンツは読み出し不能である旨通知する。このようにして、コンテンツの使用権を、そのコンテンツに関し権利を有する者の権利を犯すことなく、有効に委譲することができる。

【0032】

ここで、上記実施形態では、簡単のため、使用権情報は、使用権が存在することをあらわす‘1’と使用権が存在しないことをあらわす‘0’との二値情報で

あるとして説明したが、使用可能回数を使用権情報として用いてもよい。例えば委譲前の第1の記憶媒体10の使用権情報が使用可能回数10回をあらわす‘10’であったものとし、その使用可能回数の一部、例えば使用可能回数3回分のみを第2の記憶媒体30に委譲してもよい。この場合、第2の記憶媒体30の使用権情報は使用可能回数3回をあらわす‘3’となり、第1の記憶媒体10には、使用権情報として、使用可能回数7回をあらわす‘7’が書き戻される。第1の記憶媒体10あるいは第2の記憶媒体30でそのコンテンツが使用されると、その使用のたびに、第1のドライブに搭載された第1のファームウェアあるいは第2のドライブに搭載された第1のファームウェアにより、その第1の記憶媒体10あるいは第2の記憶媒体30の使用可能回数が1ずつ減算される。

【0033】

ここで、第2の記憶媒体30に委譲した3回分の使用権を使い切ってしまったとき、第1の記憶媒体10に未だ使用権が残っていればその使用権の一部もしくは全部を上記と同一の手順で再度第2の記憶媒体に委譲することもできる。ただしその場合は、暗号化されたコンテンツ自体は既に第2の記憶媒体30に移っているため、そのコンテンツ自体を第2の記憶媒体30に移す必要はなく、そのコンテンツの使用権のみを第2の記憶媒体30に移せばよい。

【0034】

尚、図2に示す例では、鍵1と使用権情報との双方を1つの情報と見なして、その情報を鍵2で暗号化することにより第1の記憶媒体10用の暗号化セキュア情報を生成し、鍵1と使用権情報との双方を1つの情報とみなしてその情報を鍵3で暗号化することにより第2の記憶媒体30用の暗号化セキュア情報を生成しているが、鍵1と使用権情報は、別々に暗号化してもよい。その場合、使用権の委譲にあたって鍵1は既に暗号化された形式で第1の記憶媒体10に格納されているため、新たな使用権情報のみを暗号化して第1の記憶媒体10に書き戻せばよい。また、使用可能回数を複数回に分けて委譲する場合、2回目以降の委譲の際は、第2の記憶媒体30には鍵1が鍵3で暗号化された形式で既に格納されているため、委譲を受けた使用可能回数をあらわす使用権情報のみを鍵3で暗号化してセキュアエリア32に書き込めばよい。

【0035】

また、鍵1と使用権情報のほか、例えばそのコンテンツの名称、そのコンテンツの最終アクセス日時等そのコンテンツの使用権情報以外の属性も一緒にセキュアエリアに格納してもよく、その場合に、それらの属性が暗号化する必要がないものである場合は平文のまま格納してもよく、あるいはそれらの属性が暗号化する必要がないものであっても、鍵1や使用権情報と一緒に暗号化してもよい。

【0036】

さらに、上記では使用権情報として、使用権の有無と、使用回数を取り挙げて説明したが、そのほかにも、使用可能時間を使用権情報としてもよく、アクセスが許諾された人をあらわすIDを使用権情報としてもよく、使用権の有無、あるいは使用可能範囲をあらわす種々の情報を使用権情報として使用することができる。

【0037】

図3は、本発明のライセンス委譲装置の一実施形態が搭載されたコンピュータシステムの一例を示す外観斜視図、図4は、そのコンピュータシステムの構成を示すブロック図である。

このコンピュータシステム50は、外観上は、図3に示すように、CPUやメモリ等が内蔵された本体部51、表示画面52a上に画像を表示する画像表示装置52、このコンピュータシステム50に対し各種の指示を行なうための操作子であるキーボード53、および画像表示装置52の表示画面52a上の位置を指定するための操作子であるマウス54により構成されている。また本体部51には、MO（光磁気ディスク）100が装填、取出し自在に装填されるMO装填口51aが示されている。

【0038】

また、このコンピュータシステム50は、内部構成上は、図4に示すように、各種のプログラムが実行されるCPU55、実行されるプログラムやデータの一時的な格納領域として使用されるメモリ56、キーボード53との間でデータの受け渡しを行なうキーボードインターフェース57、マウス54の操作に伴うデータを伝えるマウスインターフェース58、画像表示装置52に表示用のデータ

を伝える表示インターフェース 59、図 3 に示す MO 装填口 51 から装填された MO 100 を駆動する MO ドライブ 60、および内蔵されたハードディスク 62 を駆動するハードディスクドライブ 61 が備えられており、それらは、図 4 に示すように、バス 63 で互いに接続されている。

【0039】

ここでは、図 3、図 4 に示すコンピュータシステム 50 内において、MO 100 に格納されたコンテンツの使用権をハードディスク 62 に委譲する場合を説明するが、使用権の単純な移動、あるいは、使用可能回数が設定されている場合において、その使用可能回数以内の一部の使用可能回数を初回に委譲する場合については、図 1、図 2 を参照して既に説明済であるため、以下では、初回に委譲した使用可能回数を使い果たし、所定の使用可能回数を再度委譲する場合について説明する。また、図 1、図 2 を参照した説明は、本発明の理解のために概念的な説明を行なったが、ここではより詳細な説明を行なう。

【0040】

図 5 は、MO 100 に格納されたコンテンツの使用権をハードディスク 62 に委譲する手順を示す図である。

この図 5 には、アプリケーション 64 とドライブ 20 が示されている。アプリケーション 64 は、CPU 55 で実行される、コンピュータシステム 50 の操作者により直接に操作が可能なプログラムであって、ここでは、MO 100 内のコンテンツの使用権をハードディスク 62 に委譲することを指示するプログラムをあらわしている。また、ドライブ 20 は、ここでは、図 4 に示す MO ドライブ 60 とハードディスクドライブ 61 との複合体である。MO 100 に格納されたコンテンツの使用権をハードディスク 62 に委譲する手順を以下に説明するが、ここでは MO 100 に、委譲しようとしているコンテンツを残り 10 回使用することが出来る使用権が残っており、そのうちの 3 回の使用権をハードディスク 62 に委譲するものとして説明する。

【0041】

ここでは簡単のため、委譲され得るコンテンツは 1 つのみ存在するものとし、コンテンツと称するときは、その委譲される（あるいはその委譲によりハードウ

エア 62 に使用権が移った) コンテンツを意味するものとする。

(1) 先ず、アプリケーション 64 からドライブ 20 に向けて、コンテンツの委譲元が MO100 であり、コンテンツの委譲先がハードディスク 62 であることを、ドライブ 20 に向けて指定する (図 5 (A))。

【0042】

(2) するとドライブ 20 は、MO100 およびハードディスク 62 をアクセスするための準備を行ない、ドライブ 20 は、それらの準備が整った段階で、アプリケーション 64 に対し準備が整ったことを報告する (図 5 (B))。

(3) すると、アプリケーション 64 では、ドライブ 20 がアプリケーションに送る情報を隠蔽するためのパスワードをドライブ 20 (MOドライブ 60 とハードディスクドライブ 61 との双方) に送るとともに、MO100 のセキュアエリア (図 1, 図 2 参照) に格納されている使用権情報 (ここでは、上述の前提どおり、使用可能回数をあらわす情報を使用権情報としており、MO100 には、現在 10 回使用可能であることをあらわす使用権情報 '10' が格納されているものとする) を読み出す命令をドライブ 20 に向けて発行する (図 5 (C))。

【0043】

(4) すると、ドライブ 20 を構成する MOドライブ 60 (図 4 参照) 内では、以下の処理が実行される。ここで、MOドライブ 60 内にも CPU が搭載されており、さらに、装填された MO100 をアクセスするためのマイクロプログラムが搭載されており、それら MOドライブ 60 のハードウェアとソフトウェアとを合せたファームウェアが MOドライブ 60 における処理を実行することになる。

【0044】

(4-1) MO100 の MID エリア (図 1, 図 2 の MID エリア 11 参照) から MO100 のメディア ID を読み出す。

(4-2) MO100 のセキュアエリア (図 1, 図 2 のセキュアエリア 12 参照) から、メディア ID で暗号化された使用権情報を読み出す。

(4-3) その読み出した使用権情報をメディア ID で復号化する。

【0045】

(4-4) 上述(3)のステップにおいてアプリケーション64から送られてきたパスワードで、復号化された使用権情報をエンコードする。

(4-5) そのエンコードされた情報をアプリケーション64に伝える(図5(D))。

(5) すると、アプリケーション64は、以下の処理を実行する。

【0046】

(5-1) MOドライブ60から送られてきた使用権情報をパスワードでデコードする。

(5-2) そのデコードされた使用権情報があらわす使用可能回数がこれ以上使用できないことをあらわす‘0’でないことを確認する(ここでは、説明の前提として使用可能回数10回をあらわす‘10’が設定されており、‘0’ではない)。

【0047】

(5-3) 今度は、ドライブ20に向けて、使用権の委譲先であるハードディスク62の、使用権情報を読み出す命令を発行する(図5(E))。尚、前述したように、ここでは説明の前提として、ハードディスク62には、前回、コンテンツを何回か使用することのできる使用権が設定され、その使用可能回数が‘0’になった場合を想定している。

【0048】

(6) すると、ハードディスク62を駆動するハードディスクドライブ61では以下の処理が実行される。ハードディスクドライブ61にもCPUやマイクロプログラムが備えられており、ハードディスクドライブ61における処理も、MOドライブ60における処理と同様、それらハードウェアとソフトウェアとの複合体としてのファームウェアにより実行される。

【0049】

(6-1) ハードディスク62のMIDエリア(図1, 図2のMIDエリア31参照)からハードディスク62のメディアIDを読み出す。

(6-2) ハードディスク62のセキュアエリア(図1, 図2のセキュアエリア32参照)から、ハードディスク62のメディアIDで暗号化された使用権情

報を読み出す。

【0050】

(6-3) その読み出した使用権情報を、ハードディスク62のメディアIDで復号化する。

(6-4) 上述の(3)のステップにおいてアプリケーション64から送られてきたパスワードで、その復号化された使用権情報をエンコードする。

(6-5) そのエンコードされた使用権情報をアプリケーション64に伝える(図5(F))。

【0051】

(7) すると、アプリケーション64は、以下の処理を実行する。

(7-1) ハードディスクドライブ61から送られてきた使用権情報をパスワードでデコードする。

(7-2) そのデコードされた使用権情報が使用可能回数‘0’をあらわしていることを確認する。

【0052】

もし使用可能回数が‘0’でなく、まだ使用可能であることをあらわしているときは、本実施形態では、まだ使用可能である旨表示画面52a(図3参照)に表示してオペレータにその旨通知し、この段階で処理を中断する。

ここでは説明の前提として使用可能回数は‘0’であり、この場合、さらに以下の処理に進む。

【0053】

(7-3) ハードディスク62に新たに設定される使用可能回数(ここでは説明の前提に基づいて3回)をあらわす情報(新回数情報と称する)をパスワードでエンコードしてドライブ20(MOドライブ60とハードディスクドライブ61との双方)に送る(図5(G))。

(8) MOドライブ60では、この新回数情報を受けて以下の処理が実行される。

【0054】

(8-1) MO100のメディアIDを読み出す。

(8-2) MO100のセキュアエリアに格納されている、MO100のメディアIDで暗号化された状態の使用権情報を読み出す。

(8-3) その暗号化された使用権情報をMO100のメディアIDで復号化して使用可能回数‘10’を取り出す。

【0055】

(8-4) アプリケーション64から送られてきた、パスワードでエンコードされた新回数情報を、上述の(3)のステップで送られてきているパスワードでデコードして使用可能回数‘3’を取り出す。

(8-5) MO100にそれまで格納されていた使用可能回数‘10’からハードディスク62に譲渡しようとしている使用可能回数‘3’を差し引いて新たな使用可能回数‘7’を得る。

(8-6) その新たな使用可能回数‘7’をあらわす新たな使用権情報をMO100のメディアIDで暗号化する。

【0056】

(8-7) その暗号化された新たな使用権情報を、それまでMO100に格納されていた、使用可能回数‘10’をあらわす使用権情報に上書きする。これにより、MO100には使用可能回数‘7’が設定される。

(9) 一方、ハードディスクドライブ61では、上述の(7-3)のステップで送られてきた新回数情報を受けて、以下の処理が実行される。

【0057】

(9-1) ハードディスク62のメディアIDを読み出す。

(9-2) アプリケーション64から送られてきた、パスワードでエンコードされた新回数情報を、上述の(3)のステップで送られてきているパスワードでデコードして使用可能回数‘3’を取り出す。

(9-3) そのデコードにより取り出された使用可能回数‘3’をあらわす新たな使用権情報をハードディスク62のメディアIDで暗号化する。

【0058】

(9-4) その暗号化された新たな使用権情報を、ハードディスク62に格納されていた、使用可能回数‘0’をあらわす使用権情報に上書きする。これによ

り、ハードディスク 62 には、使用可能回数 '3' が設定される。

(10) 以上の使用権委譲の処理が完了したことが、ドライブ 20 からアプリケーション 64 に通知される。

【0059】

以上のようにしてコンテンツの使用権の委譲（ここでは使用権の一部の委譲）が行なわれる。

尚、図 5 を参照した以上の説明では、MO100 からハードディスク 62 への、コンテンツ自体および暗号化されたコンテンツを復号化するための鍵の移動については言及されていないが、前述したように、ここでは、コンテンツの使用可能回数の再度の設定の場合を説明しており、したがってコンテンツ自体および、それを復号化するための鍵は初回の委譲時に既にハードディスク 62 に渡されていることを前提としている。コンテンツ自体は、MO100 から初回の委譲時に暗号化された形式のままハードディスク 62 に移動（複製）されており、また上記の説明は、鍵はそれぞれのメディア ID で使用権情報とは独立に暗号化されてそれぞれのセキュアエリアに格納されていることを前提としている。

【0060】

尚、図 5 を参照して説明した実施形態では、上述したように、アプリケーション 64 とドライブ 20 とが様々なコミュニケーションを行ないながらコンテンツの使用権の委譲の処理を進めているが、このようなコンテンツ委譲処理に代え、アプリケーション 64 からは、使用権を委譲しようとしているコンテンツ、そのコンテンツの使用権の委譲元（ここでは MO100）、委譲先（ここではハードディスク 62）、および委譲しようとしている、使用権の回数を指定し、その後はドライブ 20（ここでは MO ドライブ 60 とハードディスクドライブ 61 との双方）に処理を任せ、アプリケーション 64 とは独立にドライブ 20 において上記の委譲処理を実行し、委譲処理が終了した段階、および何らかの不都合により委譲処理が正常に行なわれなかった（例えば MO100 に委譲を指定された使用可能回数未満の使用可能回数しか残っていなかった、あるいはハードディスク 62 に前回に委譲を受けた使用可能回数がまだ '0' になっていなかった、など）ときのみ、アプリケーション 64 に報告するように構成してもよい。

【0061】

また、上記の委譲処理60は、上記の説明ではMOドライブ60とハードディスクドライブ61とで分担して実行しているが、それらMOドライブとハードディスクドライブ61とのうちの一方はアクセス専用とし、上記の委譲処理は、専らもう一方の側で行なうように構成してもよい。

図6は、本発明のライセンス委譲装置の一実施形態が組み込まれたコンピュータネットワークの一例を示す図、図7は、そのコンピュータネットワークを構成するあるコンピュータシステムから別のコンピュータシステムに対し、コンテンツの使用権を委譲する際の手順を示す図である。

【0062】

ここには、コンテンツ管理用のコンピュータシステム70と、コンテンツを使用する側の2台のコンピュータシステム80、90が示されており、それら3台のコンピュータシステム70、80、90は、通信回線200を介して互いに接続されている。

各コンピュータシステム70、80、90は、それぞれが図3に示すコンピュータシステム50と同様の構成を備えている。すなわち、各コンピュータシステム70、80、90は、各本体部71、81、91、各画像表示装置72、82、92、各キーボード73、83、93および各マウス74、84、94を備えており、さらに各コンピュータシステム70、80、90は、それぞれが図4に示す内部構成と同様の内部構成を備えている。詳細説明は省略する。

【0063】

ここでは、コンテンツ管理用のコンピュータシステム70は、ある会社の本店に設置され、コンテンツを使用する側のコンピュータシステム80、90はその会社の各支店に設置されているものとする。以下では、説明の簡単のため、本店、および各支店に設置されたコンピュータシステム70、80、90を、そのまま本店70、支店80、支店90と称する。

【0064】

ここでは本店で、各種のコンテンツの全支店分のライセンスを購入し、その本店から各支店にライセンスを分配し、かつ、その本店で全支店分のライセンスを

管理しているものとする。すなわち、ここでは、同一のコンテンツであっても本店において必要な数の使用権を購入し、そのコンテンツを必要とする支店にその使用権を分配する。ここでいう同一のコンテンツについての必要な数の使用権は、そのコンテンツの使用回数を意味するものではなく、同一の本を複数冊（例えば3冊）購入するのと同様に同一のコンテンツの使用権を必要に応じた数だけ購入し、ここではその購入した数の使用権を意味している。本店では、各コンテンツについて、購入した使用権の数から支店に対し使用権を頒布した数の残りの数が管理されており、各支店では、同一のコンテンツについての複数の使用権は不要であって、各コンテンツについて自分の支店に使用権が存在するか否かのみを管理している。本店および各支店では多数のコンテンツの使用権情報が管理されており、ここではそれら多数のコンテンツの使用権情報の一覧を‘許諾情報’と称する。

【0065】

ここでは、本店70から各支店80、90に対し、既に様々なコンテンツの使用権が委譲されており、さらに今回、本店70からある支店（ここでは支店80とする）に対しあるコンテンツの使用権を委譲するものとし（ここでは、使用権の新たな委譲を行なおうとしているコンテンツを‘新コンテンツ’と称する）、ここでは、その新コンテンツの使用権を支店80に委譲する場面について説明する。ここでは、新コンテンツの使用権は、本店70のハードディスクから支店80のハードディスクに委譲されるものとする。

【0066】

（1）まず本店70から支店80に向けて新コンテンツの使用権を委譲する旨連絡する（図7（A））。

（2）すると支店80ではその連絡を受けて、支店80のハードディスクを準備状態にし、アクセスの準備が整うと本店70に対し準備ができたことを報告する（図7（B））。

【0067】

（3）すると本店70では、支店80から送られてくる情報を隠蔽するためのパスワードを支店80に送出し、さらに支店80のハードディスクのセキュアエ

リアに格納されている許諾情報（複数のコンテンツそれぞれの使用権の有無をあらわす情報の一覧）を送るよう命令を発行する（図7（C））。

（4）支店80では、この命令を受けて以下の処理を実行する。

【0068】

（4-1）支店80のハードディスクのメディアIDを読み出す。

（4-2）支店80のハードディスクのセキュアエリアから、そのハードディスクのメディアIDで暗号化された許諾情報を読み出す。

（4-3）その読み出した許諾情報を読み出したメディアIDで復号化する。

（4-4）上記の（3）のステップにおいて本店70から送られてきたパスワードで、その復号化された許諾情報と、さらに支店80のハードディスクのメディアIDをエンコードする。

【0069】

（4-5）そのエンコードされた許諾情報およびメディアIDを本店70に送る（図7（D））。

（5）すると、本店70では、以下の処理を実行する。

（5-1）支店80から送られてきた許諾情報およびメディアIDをパスワードでデコードする。

【0070】

（5-2）そのデコードされた許諾情報を見て、これから支店80に使用権を移そうとしている新コンテンツに関する使用権が支店80に存在しないことを確認する。これは、同一の支店に対し同一のコンテンツの使用権を重複設定するのを避けるためである。

（5-3）本店70のハードディスクのメディアIDを読み出す。

【0071】

（5-4）本店70のハードディスクのセキュアエリアから、そのハードディスクのメディアIDで暗号化された許諾情報、および、同じくそのメディアIDで暗号化された、使用権を許諾しようとしているコンテンツを復号化するための鍵を読み出す。

（5-5）その読み出した許諾情報および鍵を、読み出したメディアIDで復

号化する。

【0072】

(5-6) その復号化された許諾情報を参照して、支店80に使用権をあらたに委譲しようとしているコンテンツ（新コンテンツ）に関する使用権に残りがあることを確認する。

残りが無いときは、その新コンテンツの使用を許諾することができない旨支店80に伝えることになるが、ここでは、その新コンテンツの使用権が本店70に残っているものとする。

【0073】

(5-7) 上記の(5-1)のステップでデコードした、支店80の許諾情報中の、新コンテンツの使用権をあらわす情報を‘使用権なし’から‘使用権有り’に書き換える。

(5-8) その書き換えた許諾情報、および鍵の双方をパスワードでエンコードする。

【0074】

(5-9) 本店70のハードディスクのユーザエリアから、暗号化された新コンテンツを読み出す。

(5-10) そのエンコードされた許諾情報および鍵、および暗号化されたままの新コンテンツを支店80に送る(図7(E))。

(5-11) また、本店70内において、上記の(5-5)のステップで復号化した本店70の許諾情報中の、支店80に今回使用権を許諾した新コンテンツに関する使用権の数に関する情報を1だけ減算することにより新たな許諾情報に更新する。

【0075】

(5-12) そのようにして更新された新たな許諾情報を、本店70のハードディスクのメディアIDで暗号化する。

(5-13) その暗号化された新たな許諾情報を、本店70のハードディスクのセキュアエリアに、そこにそれまで格納されていた更新前の許諾情報に代えて格納する。

【0076】

(6) 支店 80 では、上記の (5-10) のステップで送られてきた、エンコードされた許諾情報および鍵、および暗号化された新コンテンツを受け取り、以下の処理を実行する。

(6-1) 受け取った新コンテンツを、暗号化されたまま自分 (支店 80) のハードディスクのユーザエリアに格納する。

【0077】

(6-2) 受け取った許諾情報および鍵を、上述のステップ (3) で送られてきているパスワードでデコードする。

(6-3) 自分 (支店 80) のハードディスクのメディア ID を読み出す。

(6-4) パスワードでデコードされた許諾情報および鍵を、その読み出したメディア ID で暗号化する。

【0078】

(6-5) その暗号化された許諾情報および鍵を、自分 (支店 80) のハードディスクのセキュアエリアに、それまで格納されていた許諾情報を書き換えるようにして格納する。

以上により、その新コンテンツの使用権が本店 70 から支店 80 に委譲される。

【0079】

以上の各実施形態に示すように、本発明のライセンス委譲装置は、1 台のコンピュータ等からなる 1 台の装置内においても、あるいは複数台のコンピュータ等を接続したネットワーク内においても実現可能である。

【0080】

【発明の効果】

以上説明したように、本発明によれば、コンテンツに関し権利を有する者の権利を犯すことなく、そのコンテンツを複製したり頒布したりすることができる。

【図面の簡単な説明】

【図 1】

本発明のライセンス委譲装置の一実施形態を示す構成図である。

【図 2】

図 1 に示すライセンス委譲装置の説明のための模式図である。

【図 3】

本発明のライセンス委譲装置の一実施形態が搭載されたコンピュータシステムの一例を示す外観斜視図である。

【図 4】

図 3 に外観を示すコンピュータシステムの構成を示すブロック図である。

【図 5】

MO に格納されたコンテンツの使用権をハードディスクに委譲する手順を示す図である。

【図 6】

本発明のライセンス委譲装置の一実施形態が組み込まれたコンピュータネットワークの一例を示す図である。

【図 7】

図 6 に示すコンピュータネットワークを構成するコンピュータシステムから別のコンピュータシステムに対し、コンテンツの使用権を委譲する際の手順を示す図である。

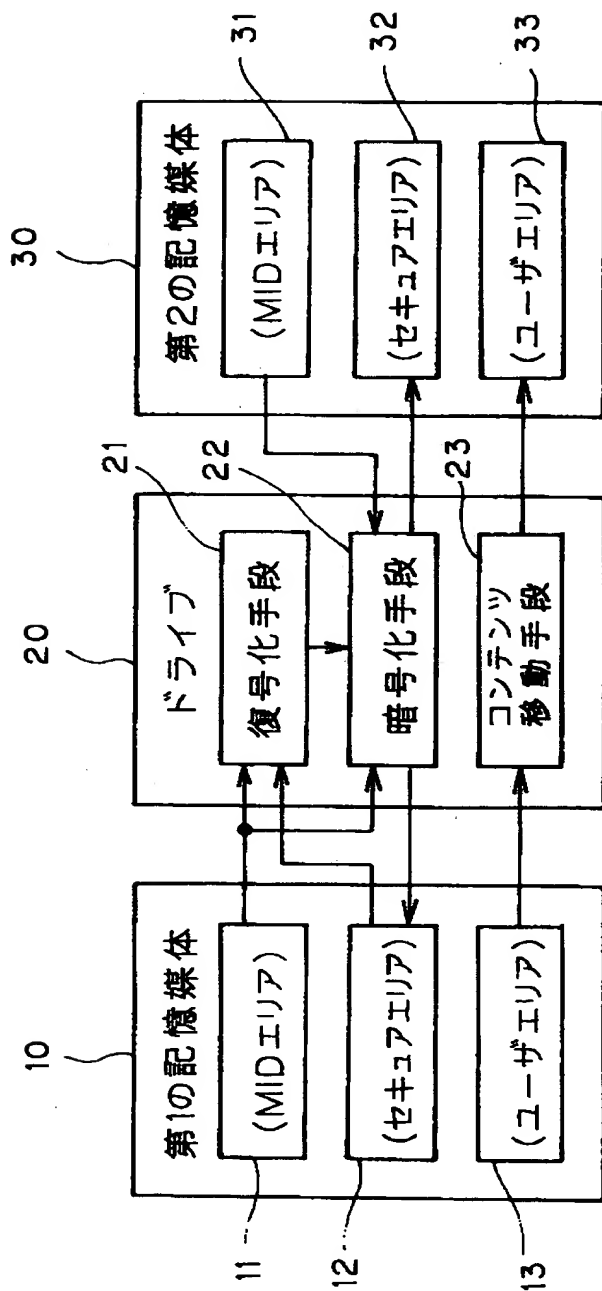
【符号の説明】

- 10 第 1 の記憶媒体
- 11 MID エリア
- 12 セキュアエリア
- 13 ユーザエリア
- 20 ドライブ
- 21 復号化手段
- 22 暗号化手段
- 23 コンテンツ移動手段
- 30 第 2 の記憶媒体
- 31 MID エリア
- 32 セキュアエリア

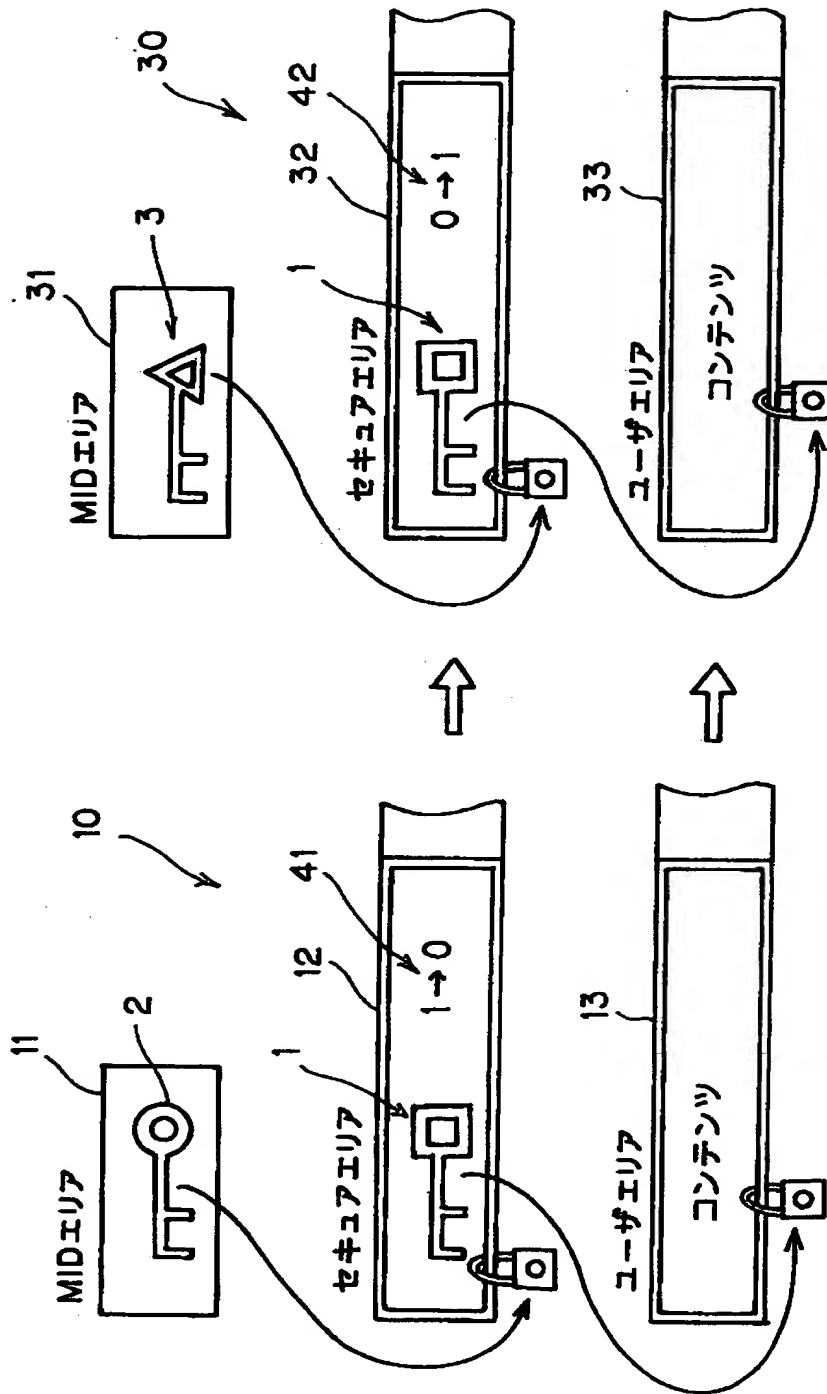
- 33 ユーザエリア
- 41, 42 使用権情報
- 50 コンピュータシステム
- 51 本体部
 - 51a MO装填口
- 52 画像表示装置
 - 52a 表示画面
- 53 キーボード
- 54 マウス
- 55 CPU
- 56 メモリ
- 57 キーボードインターフェース
- 58 マウスインターフェース
- 59 表示インターフェース
- 60 MOドライブ
- 61 ハードディスクドライブ
- 62 ハードディスク
- 70, 80, 90 コンピュータシステム
- 71, 81, 91 本体部
- 72, 82, 92 画像表示装置
- 73, 83, 93 キーボード
- 74, 84, 94 マウス
- 100 MO (光磁気ディスク)
- 200 通信回線

【書類名】 図面

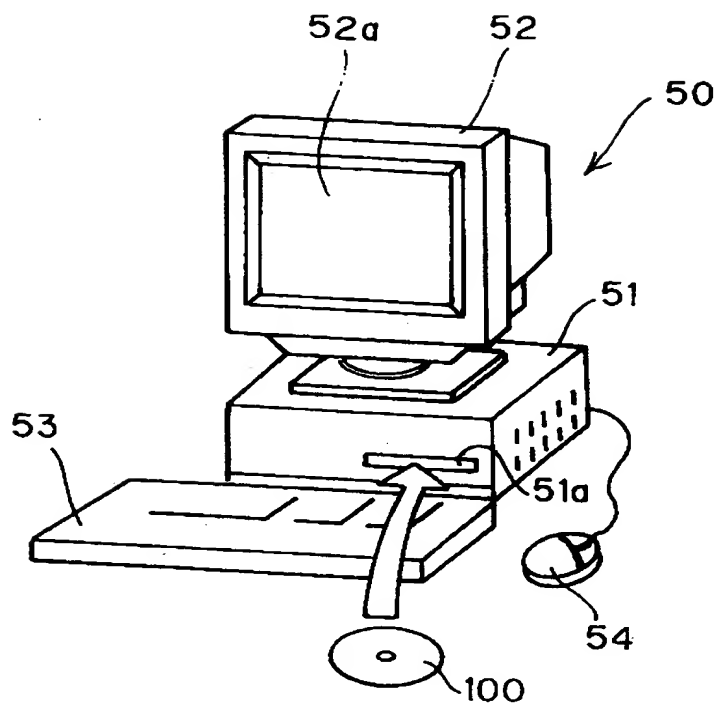
【図 1】



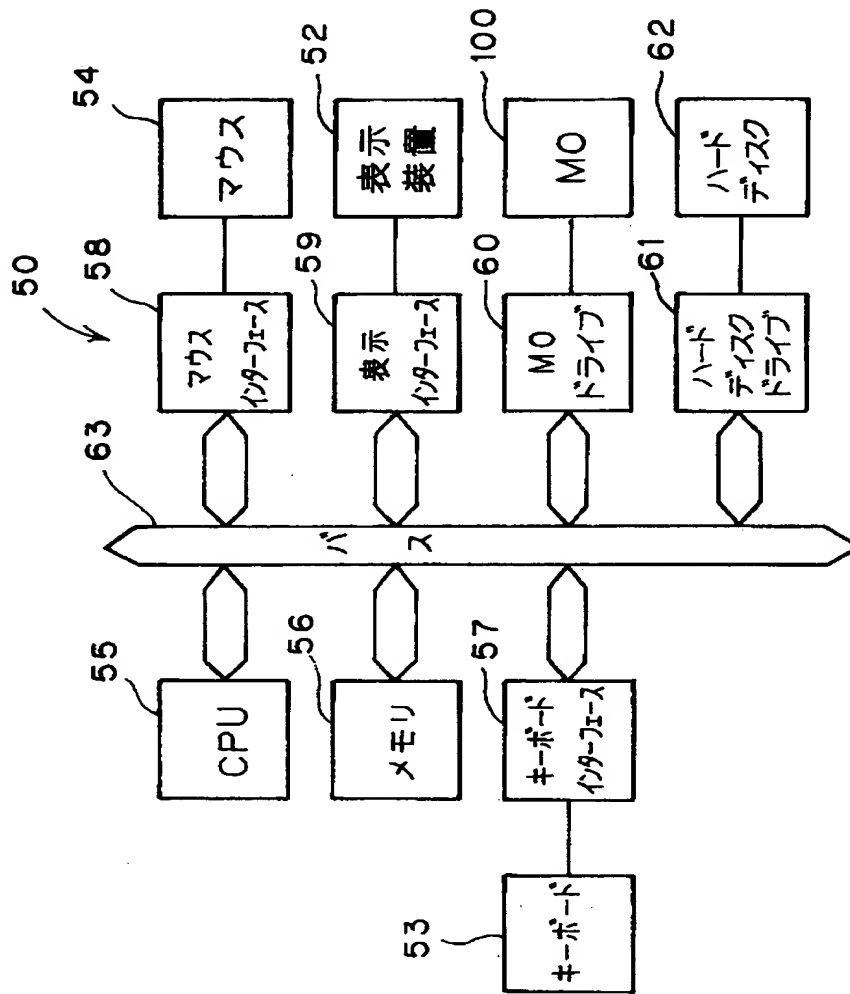
【図2】



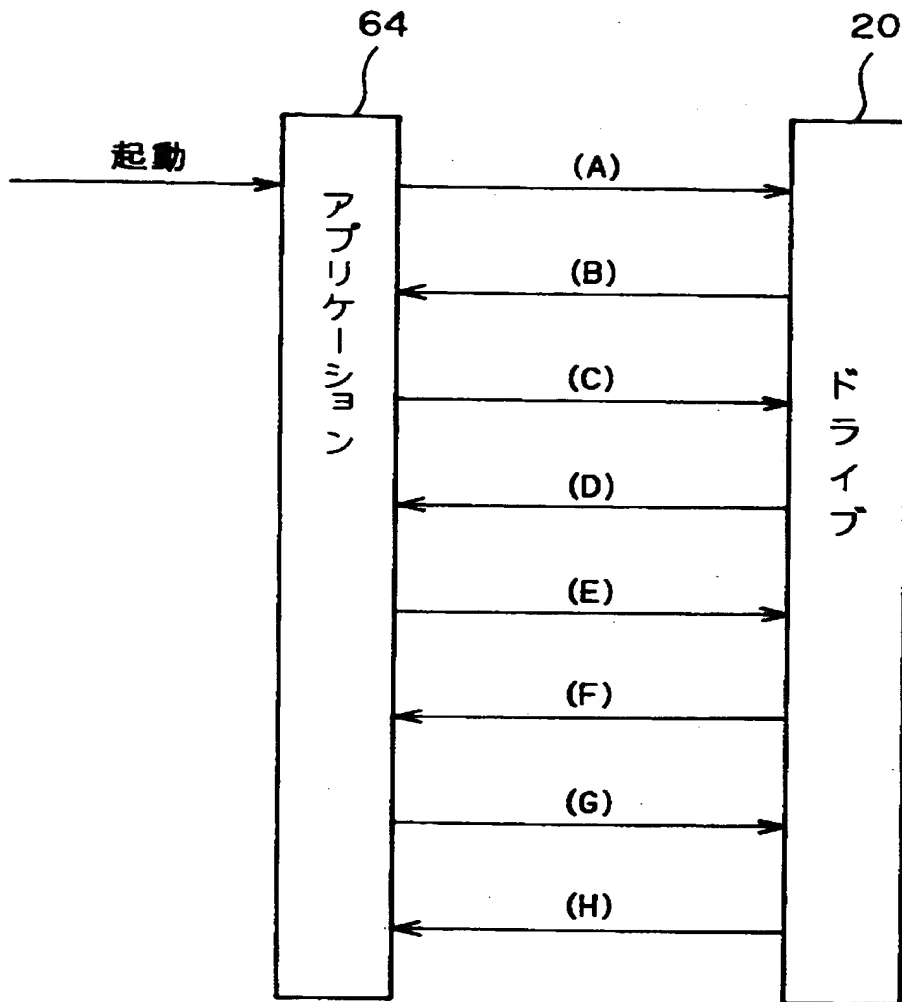
【図3】



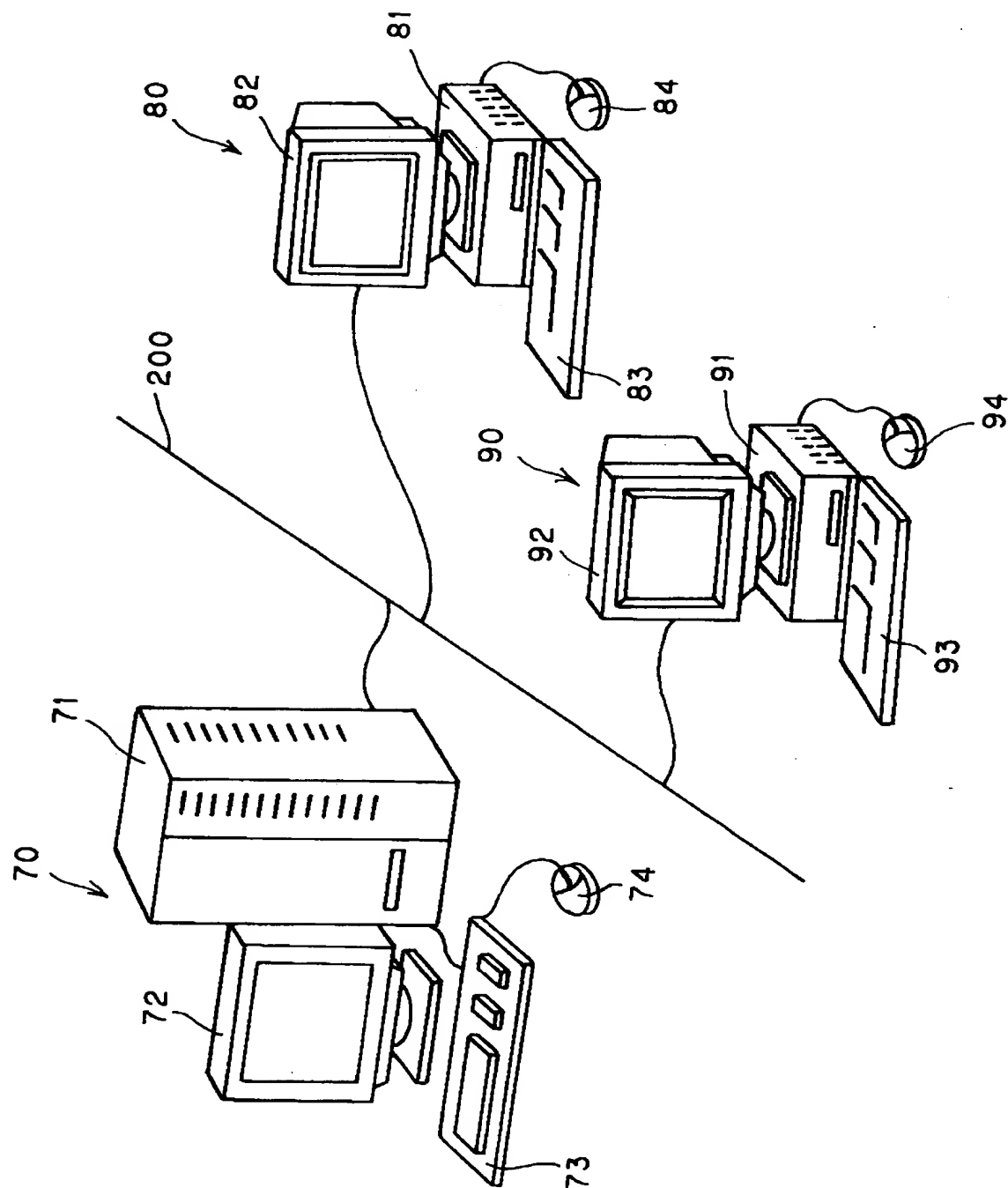
【図4】



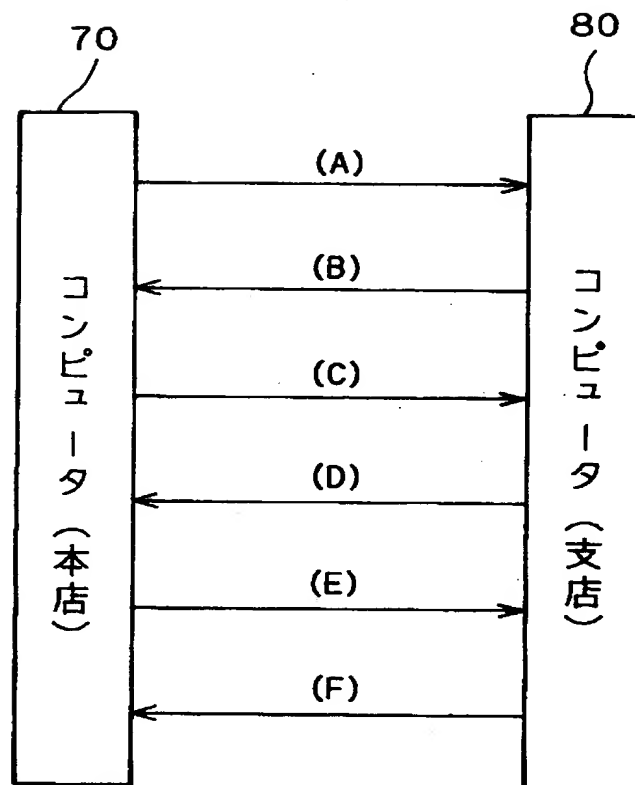
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 本発明は、コンテンツの使用権を委譲するライセンス委譲システムに関し、そのコンテンツに関し権利を有する者の保護を図りつつ、そのコンテンツの複製や頒布等を行なう。

【解決手段】 鍵 1 でコンテンツを暗号化し、その鍵 1 および使用権情報 4 1 を、それらが格納された記憶媒体 1 0 を特定するメディア ID からなる鍵 2 で暗号化しておき、そのコンテンツの使用権を委譲するにあたり、コンテンツは鍵 1 で暗号化された状態のまま、委譲先の記憶媒体 3 0 に移し、鍵 1 および使用権情報 4 1 を移転前の記憶媒体 1 0 のメディア ID で復号化し、さらに委譲先の記憶媒体 3 0 のメディア ID で暗号化して、委譲先の記憶媒体 3 0 に格納する。

【選択図】 図 1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号

【氏名又は名称】 富士通株式会社

【代理人】 申請人

【識別番号】 100094330

【住所又は居所】 東京都港区西新橋三丁目3番3号 ペリカンビル4
階 小杉・山田国際特許事務所

【氏名又は名称】 山田 正紀

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日
[変更理由] 住所変更
住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社